Monthly Security Tips
Newsletter
July 2008

CISO Tips

Remember to protect your home computer from access to unsafe and undesirable sites.
Try Blue Coat's™ free home offering at http://www1.k9webprotection.com/;

To view State security policies, please visit: http://isd.alabama.gov/policies/policies.aspx?sm=c_a;

*ALERT: please see "**New!**" security documents Guidelines 660-01S1, 660-02G5 & Policy 660-03

Web Browser Attacks

What is a Web Browser?

The Web browser is a software application that allows the user to view and interact with content on a webpage; such as text, graphics or other material.[1] It is a very popular method by which users access the Internet. There are a number of different web browsers – Internet Explorer, Firefox, Opera, and Safari are the most prevalent. Plug-ins, also known as add-ons, are applications that extend the functionality of browsers. Some of the more familiar plug-ins include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, RealOne Player and Acrobat Reader. Based on how a web page was designed, certain plug-ins may be required to view some content.

How Can Your Browser Put You At Risk?

According to a recent study, approximately 45% of people surfing the Internet were not utilizing the most secure version of their web browser.[2] Like other software, without the appropriate security patches applied, web browsers are vulnerable to attack or exploit. A fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins are not fully patched. It's important to remember that a plug-in is not automatically patched when the browser is patched.

Traditionally, browser-based attacks originated from "bad" websites but due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors.

Hackers add scripts that do not change the website's appearance. These scripts may "silently" redirect you to another web site without you even knowing about it. This redirect to another web site may cause malicious programs to be downloaded to your computer. These programs are designed generally to allow remote control of your computer by the attacker and to capture personal information – often related to obtaining credit card [or] banking information and data used for identify theft.

In April 2008 Panda Labs, a computer security and anti-virus publisher, announced that more than 280,000 web sites had been altered to redirect computers to malicious websites which would attack them in a variety of different ways. The SANS Institute, a computer security research and training organization, recently declared browser attacks to be "Top Cyber Security Menace" for 2008. It's not just desktop or laptop computers that are vulnerable. As their popularity increases, smart phones such as Blackberries®

and iPhones® may become targets of browser based attacks because of the built in browser's technology and Internet access. Clearly users must be aware of the issues and take proactive measures.

What Can You Do To Protect Yourself From Browser Attacks?

There are a number of steps that [one] can take, most of which your IT Department should have implemented at work, but which also apply equally to your home computer.

- Keep your browser(s) updated and patched
- Keep your operating system updated and patched
- Use anti-virus and antispyware software and keep them up to date
- Keep your applications (programs) updated and patched, particularly if they work with your browser such as multi-media programs used for viewing videos
- Install a firewall between your computer and the Internet and keep it updated and patched
- Block pop-up windows, some of which may be malicious and hide attacks. This may block malicious software from being downloaded to your computer
- Tighten the security settings on your browsers. Check the settings in the security, privacy, and content sections in your browser. The minimum level should be medium
- Consider disabling JavaScript, Java, and ActiveX controls

Please note a number of the above tips may impede your use of the Internet or limit what content can be accessed. If you find that ActiveX controls are needed or you require JavaScript be enabled, set the browser to prompt you before running scripts. If you find that you need to lower your security settings to be able to access what you need, lower them temporarily, then reset them.

[1] Wikipedia, http://en.wikipedia.org/wiki/Web_browser
[2] Frei, S., Dübendorfer T., Ollmann G, May M., "Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the 'insecurity iceberg' "

To learn more about Web Browser Attacks, visit the following:

- US-CERT Security Tip: http://www.us-cert.gov/cas/tips/ST05-001.html
- SANS Cyber Security Institute's Top Threats for 2008: http://www.sans.org/2008menaces/
- PC World: Hackers Increasingly Target Browsers: http://www.pcworld.com/businesscenter/article/144490/hackers_increasingly_target_browsers.html
- Computer Weekly: Attacks By Criminals on Web Browsers http://www.computerweekly.com/Articles/2008/02/14/229406/storm-worm-is-basis-for-most-cyber-attacks-says-ibm.htm
- Panda Labs: http://pandalabs.pandasecurity.com/archive/IFRAMES-Attack-_210021002100_.aspx

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture.

For more monthly tips visit: www.msisac.org/awareness/news/

http://www.msisac.org